REVISTA ESMAT
26

TECHNOLOGICAL CRIMINAL INVESTIGATION: THE ROLE OF THE TOCANTINS CIVIL JUDICIAL POLICE IN INVESTIGATING VIRTUAL RAPE

INVESTIGAÇÃO CRIMINAL TECNOLÓGICA: A ATUAÇÃO DA POLÍCIA JUDICIÁRIA CIVIL DO TOCANTINS NA INVESTIGAÇÃO DO ESTUPRO VIRTUAL

Luís Gonzaga da Silva Neto

Mestre em Prestação Jurisdicional e Direitos Humanos, pela Escola Superior da Magistratura Tocantinense (ESMAT) e Universidade Federal do Tocantins (UFT). Mestrando em Gestão de Políticas Públicas, pela Universidade Federal do Tocantins (UFT). Especialista em Ciências Criminais, pela Pontifícia Universidade Católica de Minas Gerais (PUC/Minas). Especialista em Direito de Polícia Judiciária, pela Academia Nacional de Polícia (ANP). Especialista em Gestão Política e Gestão em Segurança Pública, pela Universidade Federal do Tocantins (UFT). Graduado em Direito pela Faculdade de Alagoas (FAL). Delegado de Polícia Civil no Estado do Tocantins

RESUMO

O presente artigo analisa desafios enfrentados pela Polícia Judiciária do Tocantins no âmbito da investigação criminal do estupro virtual, o que inclui a coleta da evidência digital e demais atividades de perícia criminal. Utiliza abordagem qualitativa, por meio da análise da doutrina e jurisprudência atual sobre o tema. Os crimes que ocorriam exclusivamente no mundo físico-material migraram para o ciberespaço, o que trouxe novos desafios para sua devida adequação ilícito-típica. No caso dos crimes sexuais não foi diferente, uma vez que a gama de condutas delituosas violadoras da dignidade sexual passaram a ser cometidas em grande escala no ambiente cibernético, dentre elas o "estupro virtual". Em cotejo com o princípio da legalidade, o artigo apura se o tipo penal de estupro (arts. 213 e 217-A do Código Penal), pode se materializar no ciberespaço. Verifica obstáculos enfrentados pela Polícia Civil do Tocantins na investigação de crimes sexuais virtuais. Investiga as técnicas e as ferramentas utilizadas pela Polícia Judiciária na investigação de tais crimes. Como resultados, aponta que a doutrina e a jurisprudência admitem a prática do crime de estupro em sua forma virtual, em face da prescindibilidade do contato físico entre autor e vítima para

sua consumação, apesar da necessidade de melhor tipificação legislativa da conduta, em observância ao princípio da taxatividade. Conclui que o estupro virtual é possível devido à natureza do delito e à desnecessidade de contato corporal entre autor e vítima, embora ressalte a necessidade de aprimoramento da legislação para melhor enfrentar os desafios impostos pelos crimes cibernéticos.

Palavras-Chave: Polícia Judiciária. Polícia Civil do Tocantins. Estupro Virtual. Investigação Criminal.

ABSTRACT

This article analyzes challenges faced by the judicial police of Tocantins in the context of the criminal investigation of virtual rape, which includes the collection of digital evidence and other activities of criminal expertise. It uses a qualitative approach, through the analysis of current doctrine and jurisprudence on the subject. Crimes that occurred exclusively in the physical-material world migrated to cyberspace, which brought new challenges for their proper illicit-typical adequacy. In the case of sexual crimes, it was no different, since the range of criminal conducts that violate sexual dignity began to be committed on a large scale in the cyber environment, among them "virtual rape". In comparison with the principle of legality, the article investigates whether the criminal type of rape (arts. 213 and 217-A of the Penal Code) can materialize in cyberspace. It verifies obstacles faced by the Civil Police of Tocantins, in the investigation of virtual sexual crimes. It investigates the techniques and tools used by the judicial police in the investigation of such crimes. As a result, it points out that the doctrine and jurisprudence admit the practice of the crime of rape in its virtual form, in view of the dispensability of physical contact between author and victim for its consummation, despite the need for a better legislative typification of the conduct, in compliance with the taxation principle. It concludes that virtual rape is possible due to the nature of the crime and the lack of body contact between author and victim, although it emphasizes the need to improve legislation to better face the challenges posed by cyber crimes.

KEYWORDS: Judiciary Police. Civil Police of the State of Tocantins. Virtual Rape. Criminal Investigation.

1 INTRODUCTION

At the same time, criminals have sought to improve their criminal behavior, migrating their actions to other environments, such as cyberspace, which has become the field of action for many criminals. This fact calls for adequate preparation of police forces, whether in terms of material structure or even the training of the respective police officers, in order to ensure more efficient investigative work.

The Judicial Police must seek to act in cyberspace with investigative expertise and efficiency, as it is clear that crimes committed in the cyber environment are increasingly frequent and highly sophisticated, requiring state investigative bodies to use appropriate tools to combat this modern crime.

At the heart of crimes committed in the cyber environment, there is a debate about the possibility of committing the crime of virtual rape, and the debate revolves around the absence of physical-sexual contact between the perpetrator and the victim, as well as the possible violation of the principle of legality, specifically legal taxability, since the criminal type of the crime of rape would not cover its respective commission in cyberspace.

Furthermore, it is of the utmost importance to analyze case law in relation to the admissibility of the crime of rape in the virtual environment, looking at specific cases in Brazil and Tocantins where this possibility has been discussed. Therefore, this article will be developed by verifying the doctrine and jurisprudence in relation to the admissibility of the crimes of rape and rape of a vulnerable person in the cyber environment, being a qualitative research.

In addition, field interviews were conducted with the heads of the Cybercrime Repression Division (DRCC) and the Forensic Computing Center, both of the Civil Police of the State of Tocantins, as well as the chiefs of the 8th Specialized Police Station for Women and Vulnerable People (DEAMV) in the city of Porto Nacional/TO, and the Intelligence Division of the Institutional Intelligence and Security Center of the Court of Justice of the State of Tocantins, and the chief of the Civil Police of the State of Tocantins, with the aim of understanding the challenges faced by the Civil Judicial Police of the State of Tocantins in investigating sexual crimes committed in the cyber environment, especially the crime of virtual rape, as well as the tools available for investigative and expert investigations.

Likewise, the gathering of evidence to prove the commission of a crime is a major challenge for the Judicial Police, because we are analyzing the existence of possible obstacles to ensuring the chain of custody of digital evidence, focusing

on the structural framework and staff qualifications of the Civil Police of the State of Tocantins.

In addition, the criminal types of rape (art. 213 of the Penal Code) and rape of a vulnerable person (art. 217-A) are analyzed in terms of their compatibility with the means of execution perpetrated in the cyber environment. An improvement of the respective criminal types will be proposed, with the aim of annihilating propositions that raise a supposed violation of criminal legality in its corollary of taxability, bringing legal certainty and legal stability.

Furthermore, the issue of sexual extortion will be discussed in relation to the crime of extortion (property crime) when practiced for profit, even if the sexual crime occurs in parallel.

That said, this article deals with the concept, characteristics and classification of virtual rape, as well as presenting techniques and tools used by the Judicial Police in investigating this crime. In the same vein, the current legislation regarding the treatment of rape committed in cyberspace will be analyzed, and improvements to the legal text will be proposed with the aim of strengthening the investigation and fight against this crime.

It will also seek to identify the challenges faced by the Civil Police of the State of Tocantins in collecting digital evidence and tracking down criminals, as well as evaluating the effectiveness of the actions of the Judicial Police of the State of Tocantins in protecting victims of virtual rape.

2 ANALYSIS OF CURRENT LEGISLATION REGARDING THE CLASSIFICATION OF THE CRIME OF VIRTUAL RAPE

Sexual crimes are a very relevant topic in the context of criminal types, especially because they protect the legal asset "sexual dignity"; until recently, this group of criminal conducts was classified by the legislator as "crimes against customs". However, with the advent of Law No. 12.015 of 2009, there was a paradigmatic change in the legal and social view of this legislative spectrum, and the aspect of sexual dignity began to be taken into consideration, connecting it to the notion of human dignity, as something inherent to every human being.

When discussing the change in legislation, Masson (2018) points out that the term "crimes against customs" was excessively conservative, with the state imposing a certain standard on how society should behave in the sexual sphere, as well as proving to be quite prejudiced, with the main focus being on women.

In fact, only the so-called "honest woman" was protected by a few criminal types, with no behavioral requirements imposed on men. Law No. 12.015, of 2009, also repealed the crime of indecent assault, which was described in the art. 214 of the Penal Code. This is a purely formal repeal, since the typical conduct, in its material aspect, remained incriminated, but now under a new guise, migrating its typical elements to the crime of rape typified in the art. 213, materializing the phenomenon of normative-typical continuity.

The mentioned new legislation included the crime of rape of a vulnerable person in the art. 217-A, abolishing the presumption of violence in sexual crimes by repealing art. 224 of the Penal Code. In rape with presumed violence, the typical adequacy was mediated, since the provisions of the art. 213 were cumulated with the extension rule provided for in the art. 224 of the Penal Code.

Currently, with the changes introduced by the Law 12.015 of 2009, there are two different crimes, the incidence of which will depend on the profile of the passive subject. If the victim is a vulnerable person, art. 217-A applies; in other situations, art. 213, both of the Penal Code, apply. Analyzing the criminal types in question, it can be seen that there is no express provision for their respective practices in cyberspace. So let's take a closer look at each of them, with a view to verifying the possibility of committing them in the virtual environment.

2.1 Rape (art. 213 of the Penal Code)

The crime of rape is typified in the Article 213 of the Penal Code, which states, in verbis: "To constrain someone, by violence or serious threat, to have carnal conjunction or to practice or allow to be practiced with him another libidinous act". This is a bicommon crime, which can be committed by anyone, and does not require any specific qualities of the active subject of the crime, nor can anyone be the victim of rape.

In addition, the crime in question is material or causal, since the occurrence of a natural result is essential for its consummation. Furthermore, it is a free-form crime, as the legislator did not provide for a binding form for its practice, and it can be carried out by any means capable of causing the crime to be committed.

As has already been discussed, there is a great deal of legal controversy surrounding the feasibility of committing the crime of rape in the virtual environment, with the debate resting on (in)observance of the principle of legality. As is common knowledge, there is only a crime when it is defined by law, and if we check all the legislation, there is nothing on the crime of virtual rape.

The nomen iuris "virtual rape", according to what has already been said, is widely criticized, firstly because the crime of rape committed in the cyber environment is real conduct and not something metaphysical (virtual); secondly, rape is real because only the way it is carried out takes place in the virtual environment, and there is no emergence of new criminal conduct, not least because the incrimination of new conduct depends on a law in the strict sense.

Despite the existing problems, it is not necessary to create a new type of crime to typify the crime of virtual rape, given that the provisions of the art. 213 are sufficient to cover conduct committed in the cyber environment, especially since, as will be analyzed below, the doctrine and case law are unanimous with regard to the lack of physical-erotic contact between the perpetrator and the victim, which allows the admission of the crime at a distance, with the connectivity between perpetrator and victim through the World Wide Web.

Furthermore, in order to dispel any kind of questioning, it would be a good idea to expressly provide for the possibility of committing rape in the virtual environment, which could be provided for in the very heading of the art. 213 or even in a paragraph providing for the commission of the conduct in the virtual environment, which could be as follows: "The conduct of constraining someone, by means of a serious threat, by means of an electronic or computer device, whether or not connected to the computer network, to perform or allow a libidinous act to be performed with him, incurs the same penalty as the heading".

2.2 Rape of a Vulnerable Person (art. 217-A of the Penal Code)

The crime of rape of a vulnerable person is set out in Article 217-A of the Penal Code, which reads, in verbis: "Having carnal conjuncture or performing another libidinous act with a minor under 14 (fourteen) years of age (...) The same penalty applies to anyone who performs the actions described in the caput with someone who, due to infirmity or mental deficiency, does not have the necessary discernment to perform the act, or who, for any other cause, cannot offer resistance."

Unlike the crime of rape typified in the art. 213 of the Penal Code, rape of a vulnerable person does not include as elements of the criminal type the conduct of constraining someone by violence or serious threat; it is enough that the active subject performs a libidinous act with one of the victims set out in the incriminating provision and provided that they qualify as vulnerable.

Rape of a vulnerable person is a common crime that can be committed by anyone and does not require any specific qualities of the active subject. As far as the passive subject is concerned, it is a crime of its own, since only the person considered vulnerable can be the victim of the crime in question.

In the same way as the crime of rape in the art. 213, the crime of rape of a vulnerable person is a free-form crime, which can be committed using any means of execution. Therefore, it is fully possible to commit the crime through the virtual environment, especially as bodily contact between the perpetrator and the victim is not required, and the species is suited to the same observations outlined for the crime of rape in the art. 213 of the Penal Code.

In the case of rape of a vulnerable person, the very description of the criminal type makes it possible to commit the crime virtually, since it is enough for the perpetrator to perform a libidinous act on a vulnerable victim, without requiring any kind of constraint, even the fact that the victim consents to the act is irrelevant to the configuration of the crime, as expressly provided for in § 5 of the art. 217-A of the Penal Code.

Paragraph 5 could provide for the crime to be committed in the virtual environment, which would make it easier to accept this means of execution and remove any doubts about the possible violation of the principle of criminal legality. This way, the mentioned provision could be complemented in these terms: "The penalties provided for in the head paragraph and §§ 1, 3 and 4 of this article shall apply regardless of the consent of the victim or the fact that she had sexual relations prior to the crime, as well as the circumstance that the crime was committed by means of an electronic or computer device, whether or not connected to a computer network, to perform or allow a libidinous act to be performed with it."

2.3 Bill No. 1.891, of 2023.

Corroborating the above position, the House of Representatives Bill 1.891 of 2023 seeks to insert paragraphs 3 and 6 into articles 213 and 217-A of the Penal Code, respectively. The new provisions deal with equivalent conduct, with the following wording:

> Art. 213. (...)
>
> **Virtual Rape**

> § 3º As penas previstas neste artigo são aplicadas mesmo que o crime seja praticado à distância, inclusive pelos meios digitais, como sites da rede mundial de computadores e aplicações de internet.
>
> Art. 217- A. (...)
>
> **Virtual Rape of the Vulnerable Person**
>
> § 6º As penas previstas neste artigo são aplicadas mesmo que o crime seja praticado à distância, inclusive pelos meios digitais, como sites da rede mundial de computadores e aplicações de internet.

The purpose of these new provisions is to provide legal certainty for victims and for the Judiciary when deciding on the classification of the crime of virtual rape, not leaving decisions solely at the mercy of doctrines or case law, as well as ruling out any questioning regarding the possible violation of the principle of legality, in its taxability bias.

3 VIRTUAL RAPE

Cybercrime has been growing year after year, a fact that has been fostered by technological advances that have removed every border on the globe, making it possible for an individual living in the city of Berlin, Germany, to carry out a virtual scam to the detriment of a Brazilian victim living in the city of Araguaína-TO.

In the view of Silva Neto (2023), crime has intensified its actions in cyberspace, driven by the existing facilities, such as anonymity, which benefits the criminal, and investigative complexity. This is where the major bottleneck lies for Brazilian police forces, especially the Civil Police, which often have major problems with technological structure and personnel adequately trained to carry out investigations in the virtual environment.

Technological advances, leveraged by the spread of the Internet, have opened up a vast space for the sharing of sexual content, enabling sexual crimes to be committed in the cyber environment; when it comes to sex by text message, this circumstance is represented in the English language by the expression sexting, the result of the combination of the words sex and texting.

With regard to sexting, Machado and Pereira (2013) understand that it is an expression resulting from the combination of the words sex and texting, which in an ipsis litteris translation of the English language means sex by text message, demonstrating the problems arising from technological advances and their influence on human relationships.

In this context, the conduct of rape committed in cyberspace is covered, especially with regard to the fact that it is a free-form crime and that there is no physical-sexual contact between the perpetrator and the victim, circumstances that will be analyzed in the following topics.

3.1 A brief analysis of the possibility of typifying virtual rape

The discussion surrounding the emergence of the concept of virtual rape had its genesis in two cases that took place in the States of Piauí and Minas Gerais, both of which had the same modus operandi. In these cases, the perpetrators had intimate photos and videos of the victims in their possession, and this content was used to force them, under the threat of disclosure, to perform libidinous acts on themselves, with the aim of satisfying the lusts of the cyber criminals.

In the State of Minas Gerais, according to Vale (2017), in a report in the State of Minas newspaper, a 19-year-old man created a fake profile on a social network in order to embarrass women through threats. Initially, he persuaded the victims to send him photos and videos of pornographic content, which the victims themselves acted out.

Afterwards, the criminal blackmailed the women into sending him more intimate content, failing which he would post the photos and videos he had already received from the victims on the Internet. According to the investigations, five of the victims were aged between 16 and 24.

In the State of Piauí, according to Gomes (2017), an individual with the same modus operandi created a fake profile on Facebook, where he also influenced the victims to send him intimate photos and videos and, in possession of this content, began to embarrass them, threatening to publish everything on the Internet if they didn't send him new pornographic photos and videos. According to the investigations, the criminal demanded naked photos of the victims, inserting objects into their vaginas or even masturbating. When ordering the remand in custody, the judge explained that although there was no physical

contact between the perpetrator and the victim, the latter was forced to perform a libidinous act on herself, which clearly typified the crime of rape.

Virtual rape is represented by the conduct of an agent who, using technological means at their disposal, while the victim is physically absent, forces them by means of a serious threat to perform or allow them to perform carnal conjunction or another libidinous act. In the same vein, Meireles (2017) points out that virtual rape is nothing more than one of the types of sextortion, an expression originating from the combination of the words sex and extortion, bringing up a type of sexual exploitation in which the criminal blackmails the victim, either through an image or even a video of her in an intimate context, which can include photos in which the victim appears naked or semi-naked, or pornographic videos.

We can visualize the criminal practice in question through the following example devised by Silva Neto (2023): a woman meets a man through Facebook and starts exchanging intimate photos with him and even sending him erotic videos. At a certain point, the man the woman was in a virtual relationship with starts making threats, saying that if the woman doesn't submit to his wishes, he will publish the intimate photos and videos the victim has sent him. Trying to prevent her family and friends from having access to the material, the victim submits to the cybercriminal's threats and is forced, in a live video call, to undress and masturbate, thus satisfying the lust of the man who threatened her.

The admissibility of this crime is strengthened by the fact that there is no need for physical-erotic contact between the perpetrator and the victim, and it should be noted that rape is classified as a free-form crime, so it can be carried out by any means, and there is no specificity set out abstractly by the legislator in the descriptive criminal type.

As Silva (2020) explains, virtual rape is a consequence of the technological and social advances that have taken place in recent decades. With the area of information technology growing and presenting new ways of relating, as well as social media (WhatsApp, Facebook, Instagram etc.), the crime of rape has improved and is now practiced not only through carnal conjunction, but also through virtual space. This way of committing the crime of rape is quite recent, with few cases yet tried by the Judiciary. This can be explained by the fact that many victims are still afraid to report it, which means that this crime often occurs without being punished or even recorded.

In this way, the practice of virtual rape can be admitted, but the question arises as to a possible violation of the principle of legality, specifically in its taxability bias, in view of the absence of specific criminal typification, in which the current descriptive wording of the conduct configured as rape would supposedly be insufficient to cover the conduct practiced in the cyber environment.

In relation to the impossibility of virtual rape, due to violation of legality, Silva (2020) points out the misconception in this position, taking into account that the typical adequacy of the conduct of rape perpetrated in the virtual environment fits linearly with the criminal types described in the arts. 213 (rape) and 217-A (rape of a vulnerable person) of the Penal Code. The perpetrator, according to the author, acts intentionally, directing his actions to force the victim to perform libidinous acts under serious threat, and there is no need to speak of diversity with the typical elements of the crime of rape, fitting perfectly with the criminal type.

As such, the criminal types describing rape and rape of a vulnerable person do not hinder the practice of crime in the virtual environment, since it is a free-form crime, as explained above, and does not violate any aspect of the principle of legality; there is only one means used in the execution of the crime, in this case in a virtual way, and there is no provision for new conduct not provided for in the incriminating criminal law.

Therefore, virtual rape consists of typical conduct, in which the active subject only uses the cyber environment to commit the sexual offense in question, being fully admissible, given that it is a free-form crime and the fact that physical contact between the perpetrator and the victim is not necessary, emphasizing that the conduct takes place in the world of facts, clarifying its aspect of material crime that requires for its consummation the occurrence of the naturalistic result, that is, the practice of conjunction or another libidinous act.

It is important to state that technological means cannot be used as a shelter for criminal conduct that used to be perpetrated in the physical-material world, but which is gradually migrating to the cyber universe and deserves the criminal reprimand it deserves.

3.2 Sexual Extortion and Virtual rape

Sexual extortion is known by the term "sextortion", which originated in the United States in 2010 and it was used by the Federal Bureau of Investigation (FBI) in an investigative case in which a hacker blackmailed women by threatening to expose their privacy if they didn't comply with his demands, which consisted of sending new nude photos.

The term "extortion" refers to the property crime described in the Article 158 of the Penal Code, which makes it a crime to force someone, by means of violence or serious threat, and with the intention of obtaining an undue economic advantage for oneself or others, to do something, to tolerate doing something or to stop doing something.

In extortion, the purpose of the perpetrator is property, not sexual, which can lead to disagreements over the acceptability of so-called sexual extortion, since it is property extortion. However, if the purpose of the perpetrator is to satisfy his own lust or that of a third party, there is no need to talk about a property crime, as it is a true sexual crime.

In this context, according to Masson (2018), the crime of extortion requires, in addition to intent, a specific subjective element (special purpose of acting), which is represented by the expression "with the intention of obtaining an undue economic advantage for oneself or others", where this specific purpose differentiates extortion from the crime of rape; in the latter, the core of the type is also the verb "to constrain".

Also according to Masson (2018), in the crime of rape, unlike extortion, the constraint by violence to the person or serious threat is aimed at a sexual purpose, which can be carnal conjunction or any other libidinous act.

Therefore, if we are dealing with sexual extortion committed in the cyber environment, there is no need to talk about the crime of extortion (property crime) if the purpose that permeates the conduct of the cybercriminal has a sexual connotation, since it will be a crime against sexual dignity, as is the case with virtual rape, even if there is a secondary purpose of obtaining property profit, for example with the sale of photos and videos obtained through embarrassment perpetrated against the victim.

In view of the above, it would be a good idea to improve the legislation, emphasizing that the fact that the perpetrator aims to make a profit by obtaining intimate photos and videos of the victim would not exclude the incidence of the criminal type of sexual offense, as long as it is also aimed at satisfying his own

lust or that of a third party, which is presumed when committing the conduct described in the criminal types of rape and rape of a vulnerable person.

3.3 The crime of real rape

The crime of rape is described in the art. 213 of the Penal Code, and art. 217-A of the same law defines the crime of rape of a vulnerable person, which is also at the heart of this discussion.

The typical elements of the criminal type of rape are violence and serious threat, one or the other of which may occur as a way of enabling the constraint placed on the victim by the active subject at the time of the crime. In addition, it is important to say that in the case of rape of a vulnerable person, the elements are not present, and it is enough for the perpetrator to perform a libidinous act, carnal conjunction or a different libidinous act, with a vulnerable person, for the purposes of the typical framework.

In this context, it is important to note that rape is a free-form crime, especially with regard to the practice of a libidinous act other than carnal conjunction; therefore, it is necessary to analyze the possibility of its practice in the cyber environment, where the neuralgic point of the discussion revolves around the impossibility of physical contact between perpetrator and victim.

3.4 The lack of physical contact as a fundamental distinctive feature between real rape and virtual rape

As Gonçalves (2018) explains, physical contact between the perpetrator and the victim is not necessary for the crime of rape to occur, as the use of a serious threat to coerce the victim into self-masturbation or to use a vibrator on their genitals, for example, is sufficient for the sexual crime to be established. Therefore, what is essential for the rape to occur is the presence of the bodily involvement of the victim in the libidinous act.

According to the Superior Court of Justice (2016): "The conduct of lasciviously contemplating, without physical contact, for a fee, a minor under the age of 14 stripping naked in a motel may allow for the initiation of criminal proceedings to investigate the crime of rape of a vulnerable person." In the view of Cunha (2016), physical contact between the perpetrator and the victim is unnecessary, and the crime is configured in the conduct of the agent who determines that the

victim masturbates only for the contemplation of the active subject. In the same vein, Cavalcante (2023) argues that the mere act of the perpetrator contemplating the naked victim in order to satisfy his lust (lascivious contemplation) is sufficient to constitute the crime of rape (art. 213 of the Penal Code) or rape of a vulnerable person (art. 217-A of the Penal Code).

It is clear from the arguments raised that the definition of the crime of rape does not require physical-sexual contact between the aggressor and the victim, paving the way for the emergence of so-called "virtual rape". In this regard, Masson (2018) argues that it is fully possible to commit the crime of rape remotely, making room for the feasibility of committing it in cyberspace through the use of some electronic means (Skype, Whatsapp, Facetime, etc.).

In addition, with regard to the term virtual rape, there is some criticism within the doctrine, as is the case with Meireles (2017) and Pereira (2017), because there is a misunderstanding of the term virtual, given that it is real rape, in which the virtual aspect refers only to the mode of execution, by means of a serious threat, with the libidinous acts being practiced physically, with cyberspace functioning only as a means of interconnection between perpetrator and victim.

For Pereira (2017), the criminal type provided for in the art. 213 of the Penal Code does not include the practice of virtual rape, for whom it would be necessary to modify the legislation in order to adjust it to the new social dynamism. For this author, virtual rape would constitute a crime of illegal constraint, as typified in the art. 146 of the Penal Code.

We differ on this point, because illegal restraint is a subsidiary crime, in which its incidence is conditional on the perpetrator not committing a more serious crime. However, if the purpose of the constraint is to make the victim perform a sexual act or allow it, there is no way of admitting that the criminal type of rape is not applicable, giving way to the application of a less serious crime and a typical element of sexual crime, which would represent an inversion of the legal logic that permeates the typical-criminal incidence at the heart of the Repressive Statute of the country.

According to Martins (2017), virtual rape is nothing more than the commission of the crime of rape through the use of the Internet as a means of achieving criminal consummation, in which through the great network there is embarrassment, by means of a serious threat, so that the victim submits to the libidinous desires of the sexual cybercriminal.

Committing the crime of virtual rape only involves a serious threat, because, as Meireles (2017) points out, committing the crime by means of carnal conjuncture is unacceptable in the cyber sphere, given that the very definition of carnal conjuncture shows that physical contact is essential, with the introduction of the penis into the vagina. As for the serious threat, as explained above, it is fully applicable, and the criminal conduct is configured by the practice of any act by vis compulsiva or vis corporalis to satisfy the lust of the criminal.

Along these lines, the Superior Court of Justice (2016), in the judgment of Habeas Corpus No. 70976/MS, ruled that "the majority of Brazilian criminal doctrine is of the opinion that lustful contemplation constitutes the libidinous act that constitutes the types of articles 213 and 217-A of the Penal Code, and that physical contact between the offender and the offended is irrelevant for the consummation of the offenses."

Thus, within the scope of the second type of rape, the commission of a libidinous act other than carnal conjunction, specifically in relation to the conduct of practicing, there is no constant requirement for the physical presence of the active subject, since the implementation of the serious threat can be carried out at a distance, requiring only the involvement of the victim's body in the sexual act, providing space for the commission of this crime in the cyber environment, and there is no need to talk about the absence of legal classification or even a violation of strict legality.

4 INVESTIGATION OF VIRTUAL RAPE BY THE JUDICIAL POLICE

Contemporary crime has migrated its criminal activities to cyberspace, a movement that has posed various challenges for public security agencies, since investigations now require an extremely technical analysis, in addition to the difficulties in detecting criminal authorship, given the guarantee of impunity at the heart of cybercrime, but, as will be explained in this topic, there have been various advances in the investigative field, especially through the use of technological tools at the heart of unraveling this new form of crime.

For a long time, the Brazilian Judicial Police operated their investigations in a nuclear fashion by taking witness statements, which were the main means of obtaining evidence, with the entire investigative process based on the personal arguments and perceptions of individuals who had supposedly witnessed the commission of the crime.

Contemporary crime has started to migrate its actions from the physical world to the virtual environment, and investigative bodies have had to seek improvements in order to keep up with the advance in the practice of crimes in cyberspace.

Initially, it is of the utmost importance to analyze specific cases in which the occurrence of virtual rape has been verified, in which the investigation has seen the criminal classification, falling within the provisions of the Penal Code.

4.1 Case of virtual rape in the city of Porto Alegre, State of RS

In the city of Porto Alegre, State of RS, a 24-year-old medical student communicated with a 10-year-old boy, who lived in the city of São Paulo, State of SP, through a social network, using audio and video software. The student had sexual dialogues with the child, and some of these virtual encounters took place without the use of clothing.

The father of the child found out what was going on and immediately contacted the police who, after an in-depth investigation, managed to arrest the cybercriminal, even discovering that the suspect was storing around twelve thousand images of child pornography.

Judge Tainara Gischkow Golbert, of the 6th Criminal Court of the Central Court of the city of Porto Alegre, said in her decision: "The peculiarity of this case is that it recognizes the incidence of the criminal type of rape of a vulnerable person (article 217-A of the Penal Code), perpetrated by virtual means, since the defendant and the victim were in different States of the federation."

4.2 Case of virtual rape in the city of Teresina, State of PI

Another case of virtual rape took place in the city of Teresina, State of PI in 2017, in which a man took images of his ex-girlfriend undressing while she slept, creating a fake profile on a social network and threatening to publish the images if the victim didn't send him intimate photos.

The victim, fearing that her photos would be made public by her ex-partner, ended up agreeing to masturbate using vibrators, as well as inserting other objects into her genitals, showing the images to the criminal. In this case, the perpetrator was convicted of rape (art. 213 of the Penal Code).

4.3 Cyber-criminal investigation and the Civil Rights Framework for the Internet

In the two cases mentioned above, the police were able to identify the perpetrators by analyzing the IP numbers assigned to the computers of the criminals. Law No. 12.965, of April 23rd, 2014, which establishes the principles, guarantees, rights and duties for the use of the Internet in Brazil, known as the "Civil Mark of the Internet", defines the Internet protocol address (IP address) as the code assigned to a terminal on a network to allow it to be identified, defined according to international parameters (art. 5, item III). Therefore, the IP address makes it possible to identify the terminal used by the user, because it is assigned a code, making it possible to precisely identify the device used.

The Civil Mark of the Internet also provides for Internet application access registers, which are the set of information relating to the date and time of use of a given Internet application from a given IP address (art. 5, VIII). Therefore, it is possible to locate the IP address assigned to the terminal where the criminal conduct took place; consequently, the authority responsible for the investigation will be able to check the records of access to Internet applications that took place on a particular computer or smartphone.

Furthermore, the Internet application provider must keep the records of access to Internet applications confidential, in a controlled and secure environment, for a period of six months. In addition, a court order may oblige Internet application providers who are not subject to the aforementioned time limit to keep Internet application access logs for a certain period of time, as long as the logs relate to specific facts over a specific period of time. The police or administrative authorities or the Public Prosecution Office may request any Internet application provider to store access logs as a precautionary measure, even for a longer period than that provided for by law.

On another point, connection providers must keep connection logs under wraps, in a controlled and secure environment, for a period of one year, noting that responsibility for keeping connection logs cannot be transferred to third parties. The police or administrative authorities or the Public Prosecution Office may request that the connection logs be kept for a longer period, in which case the requesting authority will have a period of sixty days from the request to file a request for judicial authorization to access the logs.

As explained above, the Internet Protocol address (IP address) is the code assigned to a terminal on a network to allow it to be identified, defined according

to international parameters. The terminal is nothing more than the computer or any device that connects to the large network. For a terminal to connect to the Internet, it must have a connection provider who will assign or authenticate an IP address.

4.4 Important steps in the investigation of virtual rape

4.4.1 Obtaining the connection registers

Furthermore, in the context of an investigation into sexual cybercrime, it is of fundamental importance to search the entire connection log, the purpose of which is to verify to which user that IP was assigned, on the day and at the time of the crime, with the respective time zone.

According to the Civil Mark of the Internet, the connection record consists of all the information regarding the date and time of the start and end of an Internet connection, its duration and the IP address used by the terminal to send and receive data packets. The terminal is the computer or any device that connects to the Internet.

The Internet Protocol address (IP address) is the code assigned to a terminal on a network to allow it to be identified, defined according to international parameters. Therefore, for a terminal to be able to connect to the Internet, it is essential to assign or authenticate an IP address, which can be fixed, when it does not change with each connection, or a dynamic IP, when it changes with each new connection made by the user through a terminal.

In this regard, it is possible that the IP number assigned is the same for more than one user, due to the difficulties generated by the sharing of IPv4 addresses by Internet providers, specifically through the operation of CG-NAT platforms44.

The Carrier Grade Network Address Translation (CG-NAT) platform makes it possible to share public IPv4 addresses, so that several users can access the Internet from the same public IP address at the same time. It is therefore of the utmost importance that the police authority investigating a cyber sex crime asks for the logical port of the hardware, as well as the IP address used by the cybercriminal.

The exhaustion of the IPv4 has hampered investigations and there is an urgent need to implement a new version of the protocol, IPv6. With the implementation of the IPv6 there will be an abundance of IP addresses (which is not the case with

the IPv4) and it will be possible to assign a specific identifier number to each connection.

According to Pereira (2019), this sharing of public IPs between several users is a temporary solution adopted to address the shortage of the IPv4 standard IP addresses, due to the delay in migration to the updated and the new IPv6 standard.

According to Porto (2023), a network is established between users, promoted by the connection provider, which assigns them a local (private) IP address; to do this, it uses NAT to map and translate the private IP addresses of the users into valid Internet addresses (public IP addresses). The assignment of public IPs makes it difficult to identify the terminal from which the cybercrime originated, and it is of fundamental importance to carry out field diligence in order to reach the user who connected to the large network to commit the crime.

4.4.2 Obtaining records of access to Internet applications

Virtual rape is commonly practiced through the use of Internet applications such as Facebook, Instagram, WhatsApp, Twitter, Gmail, among others. According to the Brazilian Civil Rights Framework, Internet applications are the set of functionalities that can be accessed through a terminal connected to the Internet.

In this sense, the record of access to Internet applications is the set of features relating to the date and time of use of a given Internet application from a given IP address.

As far as Facebook and Instagram are concerned, access records are obtained through the online law enforcement platform Facebook Records, where it is possible to request the precautionary preservation of user profiles and their registration data, without the need for a court order.

Access to this platform is conditional on the applicant being in charge of an ongoing investigation. Furthermore, no new social network profile will be created for the applicant, only an institutional e-mail will be linked to the case that will be opened at the application provider.

Figure 1: Facebook Records[1]

Source: Meta, 2023.1

In relation to WhatsApp, the WhatsApp Records platform is used to request records of access to the application, as well as for the precautionary preservation of said user data, and it is possible to obtain user information such as: contacts, date, time and data on sending and receiving messages (IP address, mobile operator used, version and device identification number, web browser configuration information for accessing the device and location data at the time of using the services).

Figure 2: WhatsApp Records[2]

[1] Imagem capturada da página da empresa Facebook na Internet para solicitações de autoridades públicas.

[2] Imagem capturada da página da empresa WhatsApp na Internet para solicitações de autoridades públicas.

When committing the crime of virtual rape and other sexual offenses in the cyber environment, cybercriminals create fake profiles on social networks, especially Facebook and Instagram, through which they lure their victims, obtain photos and videos of erotic content, and blackmail them by threatening to disclose the content, making non-disclosure conditional on sending more and more photos and videos of the same nature.

4.4.3 Virtual infiltration

On the other hand, there is the virtual infiltration of agents, which is a precautionary evidentiary measure and an important investigative means, whose object of investigation is specific crimes, whether involving criminal organizations or crimes typified in the Law No. 8,069, of 1990 (Statute of the Child and Adolescent), or in the Penal Code.

Virtual infiltration will always be preceded by a duly detailed and reasoned judicial authorization, which will establish the limits of the infiltration in order to obtain evidence. It will also take place at the request of the State Prosecution or a representation of the police officer, and will contain a demonstration of its necessity, the scope of the tasks of the police officers, the names or nicknames of the people being investigated and, where possible, the connection or registration data that will allow these people to be identified. Police agents will

not be allowed to infiltrate the Internet if the evidence can be obtained by other means, as this is a measure of ultima ratio.

An important point is that there is no provision for infiltration by intelligence agents belonging, for example, to the Brazilian Intelligence System (SISBIN) or the Brazilian Intelligence Agency (ABIN). This is because infiltration is a measure for gathering evidence, and is not an intelligence activity, since the latter aims to produce knowledge to support the decision-maker.

Among the crimes provided for in the art. 190-A of the Law no. 8,069 of 1990, which allow for the virtual infiltration of agents, there is the express provision for rape of a vulnerable person (art. 217-A of the Penal Code), showing that even the legislator explicitly recognizes the possibility of rape of a vulnerable person committed in the virtual environment. Likewise, although not provided for in the aforementioned provision, we can also conclude that the crime of rape (art. 213 of the Penal Code) is tacitly admitted in the cyber environment.

With regard to the infiltration, Lopes (2011) states that the undercover agent is a member of the police, who acts with prior judicial authorization, concealing his identity, in which he inserts himself in a stable way in a certain criminal organization, in which he acquires the trust of the respective members, and with this, having access to confidential information, ensures the identification of criminals and the crimes they perpetrate.

According to Sato (2013), the infiltration of agents in the virtual environment is one of the ways of operationalizing agent infiltration, in which the police officer can create a fictitious profile, through which he can maintain contact with those suspected of committing virtual sex crimes against children and adolescents, making it possible for him to participate in forums and discussion groups, in which he will disguise his identity, the main purpose of which is to gather information related to the criminal system developed by those being investigated.

Virtual infiltration can also be called light cover, which is a less incisive form of infiltration. At this point, according to Silva (2016), the creation of a false user profile (fake profile creation), with the concealment of the true personality of the investigator on the Internet, is classified by the American doctrine as light cover infiltration operations, falling under a soft infiltration, of short duration, not requiring the infiltrated agent to be continuously and permanently immersed, requiring less complex planning.

4.4.4 Use of geolocation in investigations

Another important investigative tool is the geolocalized search for posts using the Skylens platform, which, according to Caselli (2023), creates an electronic fence in the search for posts with an indication of geolocation on the social networks Twitter, YouTube, Instagram, among others, being efficient in relation to the reach of posts from open, non-private profiles, with the result being an interactive map with the indication of the post, the date and the location indicated by the user of the profile.

In sextortion, criminals often post photos and videos of their victims on fake profiles, but these are open (non-private) social media pages, which allows for investigative success through the use of the geolocation tool.

5 CYBER INVESTIGATION WITHIN THE SCOPE OF THE CIVIL JUDICIAL POLICE OF THE STATE OF TOCANTINS

In the state of Tocantins, the Civil Police, through its Superior Police School (ESPOL), has implemented a series of training courses for police officers in the area of cyber investigation, seeking to bring efficiency and solidity to the wide range of cyber crime cases that arrive daily at police stations throughout the State of Tocantins.

In recent years, the Superior Police School has offered courses focusing on cybercrime investigation, such as: a) technological criminal investigation; b) intelligence and criminal investigation in open sources; c) precautionary measures in the context of cyber investigations; d) technological tools for extracting data from electronic devices; e) data processing; among other subjects inherent to the theme in question.

Furthermore, the Civil Police of the State of Tocantins has been making progress in the investigation of sexual cybercrimes, including virtual rape, as well as in the field of computer forensics, since the success of investigations involving crimes committed in the virtual environment is intrinsically linked to the solidity of the forensics work at the heart of the chain of custody of digital evidence and the extraction of data from electronic devices.

Having said that, we will now analyze important aspects of criminal forensics and the investigation of sexual crimes committed in the virtual environment; to this end, we will use data and information gathered in interviews with the heads

of the Cybercrime and Repression Division and the Forensic Computing Center, both sectors within the structure of the Civil Police of the State of Tocantins.

5.1 Cyber Investigation of Virtual Rape in the State of Tocantins

In the State of Tocantins, the Cybercrime Repression Division (DRCC), located in the city of Palmas and headed by Police Chief Lucas Brito Santana, uses investigative techniques to uncover virtual sex crimes, which will be analyzed below, based on information provided by the police authority in this research.

The investigative techniques are based on the specific circumstances of each case, especially with regard to the application provider used in the crime, such as WhatsApp, Telegram, Instagram, Facebook, Skype, Tik Tok and Kwai. As Dr. Lucas Brito explains, "each of these platforms provides a range of data that enables the individualization and location of the user responsible for the criminal accesses."

It should be noted that the elements provided by the platforms mentioned above are of paramount importance for the investigation of criminal acts that occur on them, but if they are not sufficient, they can be complemented by data obtained from research carried out on open sources, monitoring of social networks, requests for registration data and judicially authorized telephone interceptions.

According to the head of the Cybercrime Repression Division of the State of Tocantins, "as is intrinsic to the investigation of any crime in the virtual environment, there is always a massive amount of data to be analysed, and some tools help to systematize the information framework, such as IPED (software used to index, process and analyse digital evidence) and IBM i2 (visual analysis software capable of gathering, displaying, cross-referencing and analysing data using diagrams)".

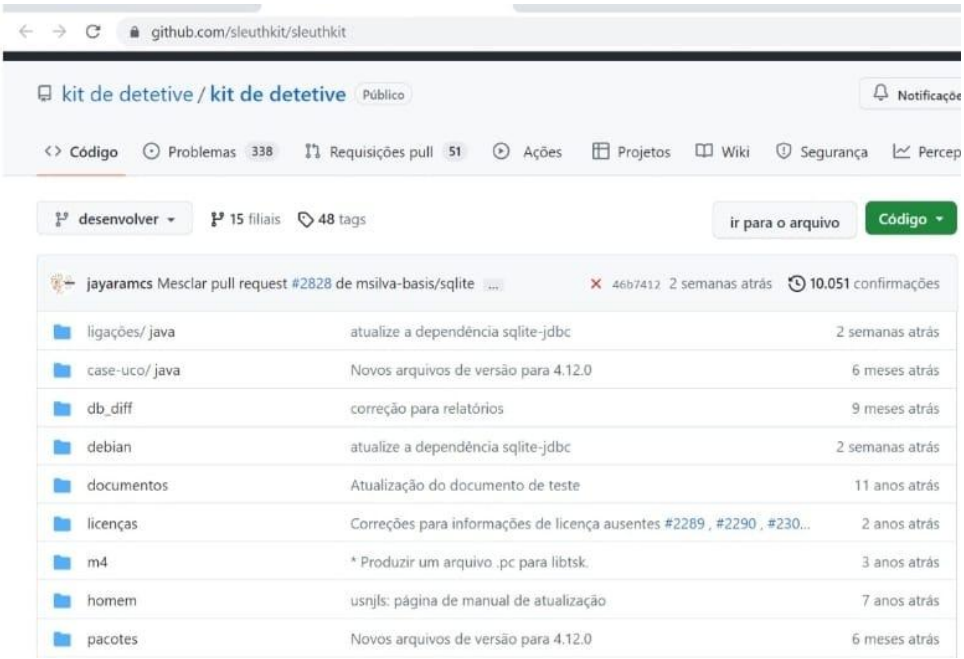
The Indexer and Processor of Digital Evidence (IPED) is a Brazilian forensic tool developed by the Federal Police in 2012, but only in 2019 it was made available to the general public, becoming a public open source project and made available on the GitHub of the Federal Police.

The Digital Evidence Indexer and Processor is implemented in java, with the aim of processing data efficiently and stably, and its main features are: (a) batch case command line data processing; (b) multi-platform support, tested on Windows and Linux systems; (c) portable cases without installation, which allows

execution from removable drives; (d) integrated and intuitive analysis interface; (e) high multithread performance and support for large cabinets, with a processing speed of up to 400 GB/h using modern hardware and 135 million items in one (multi) cabinet, as of December 12th 2019.

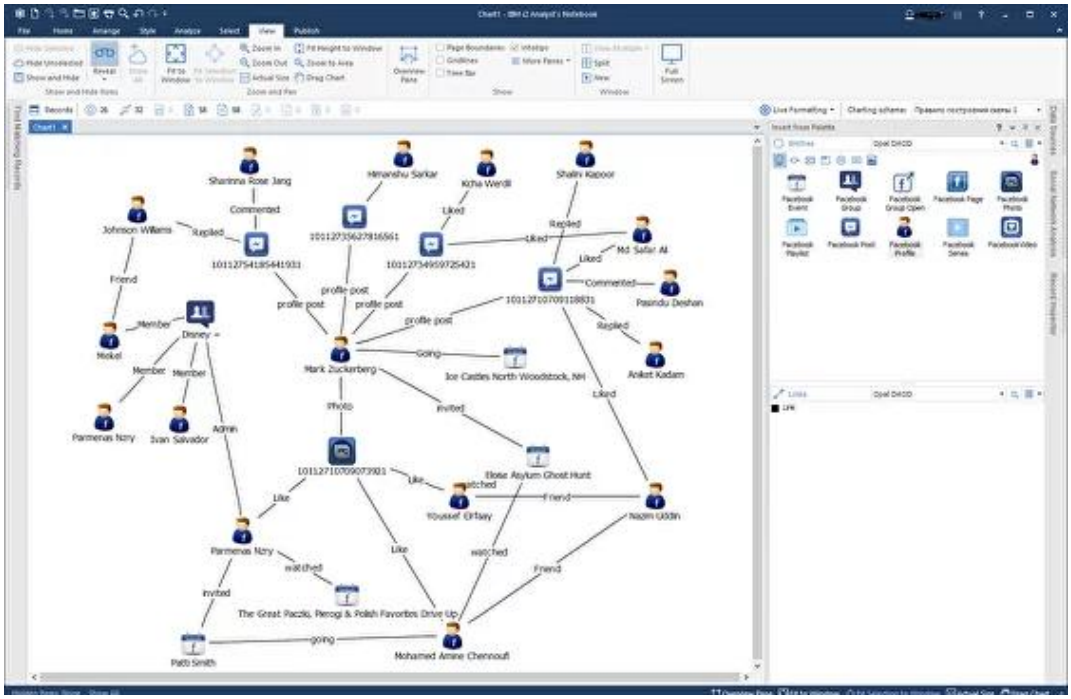
Currently, the Digital Evidence Indexer and Processor only uses the Sleuthkit Library to decode disk images and file systems, so the same image formats are supported: RAW/DD, E01, ISO9660, AFF, VHD, VMDK. EX01, VHDX, UDF (ISO), AD1 (AccessData) and UFDR (Cellebrite) formats are also supported.

Figure 3: Library *Sleuthkit*



Sourde: Github, 2023.1

Figure 4: Image of the IBM i2.



Source: Social Links, 2023.1

According to the head of the Cybercrime Repression Division in the city of Palmas/TO, with regard to the use of the investigation techniques described above, he states that

> Há êxito repressivo sempre que verificado não apenas o comprometimento dos profissionais envolvidos diretamente nas apurações – os quais necessitam de expertise teórica e prática, além de proatividade e boa dose de obstinação –, mas também o respaldo institucional, em todas as esferas, mediante disponibilização de recursos humanos, materiais e estruturais adequados, na esteira do discorrido nas respostas precedentes. Em síntese, quando esta relação está desequilibrada, surgem as sobrecargas e, por consectário, os gargalos investigativos (Santana, 2023).

Next, we will analyze some cases of virtual rape investigated by units of the Civil Police of the State of Tocantins, in which the police authorities who presided over the respective investigations were interviewed.

5.1.1 Virtual rape in the city of Porto Nacional/TO

In the city of Porto Nacional/TO, according to the Tocantins Conection portal (2021), a 25-year-old man was indicted by the Civil Police for the crime of virtual

rape. According to the investigations carried out by the 8th Specialized Police Station for Women and Vulnerable People, the victim met the suspect on Facebook, and during the conversations they exchanged intimate photos ("nudes").

On April 18th, 2021, the victim and the suspect decided to talk via video call, at which point the victim realized that the appearance of the man did not match the photo on his social network profile, at which point the victim informed him that she no longer wished to continue talking to him.

The suspect then proceeded to send the victim's intimate photos to her WhatsApp, threatening her that he would post the photos in chat groups if she didn't make a video call with him, in which the victim would have to show her private parts. As the victim was under serious threat from the offender, she ended up agreeing to make the video call in which she showed her private parts, with the suspect also showing himself in a situation of nudity.

The head of the 8th DEAMV, talking about the challenges of the investigation, explains:

> O estupro virtual ocorria durante as chamadas de vídeo, quando o autor obrigava a mulher a mostrar suas partes íntimas e se tocar, portanto tais chamadas não ficavam gravadas. Não obstante, havia mensagens no WhatsApp e no Instagram, nas quais o autor deixava claro que possuía as fotos íntimas da vítima, e que as divulgaria, caso a vítima não aceitasse fazer chamadas de vídeo com ele, restando configurada a ameaça. Outras mensagens indicavam o teor das chamadas, corroborando com o relato da vítima (Correia, 2023)

In the investigation, according to the head of the 8th DEAMV in the city of Porto Nacional/TO, when discussing the techniques and tools used to find the perpetrator, the contents of the cell phone of the victim were extracted. As part of the police report on the case, the links to the social networks used by the perpetrator were listed.

According to the police authority, Facebook and Instagram were contacted via the "Facebook Records" platform, as well as WhatsApp via "WhatsApp Records", in which the registration details of the accounts used by the suspect were requested. In addition, the cell phone operator was also contacted, enabling the data to be compared in order to determine the perpetrator. It was discovered that the suspect lived in the city of Natividade/TO, and thanks to the support

provided by police officers in the region, the location of the individual was obtained, and he was interrogated by the letter of request.

When asked, in the light of the investigation, what could be improved in the cybercrime investigation methodology developed by the Civil Judiciary Police of the State of Tocantins, the police officer said that at the time of the investigation she had undergone training at the Superior Police School of the State of Tocantins (ESPOL/TO), which dealt with the investigation of crimes committed in the virtual environment, which was crucial for her, because when the investigation took place she had the necessary knowledge to obtain the registration data on the aforementioned platforms, which was decisive in arriving at the perpetrator.

However, she warns of the need to extend the training in investigating virtual crimes to all other civil police officers in the State of Tocantins:

> No entanto, esse tipo de capacitação deveria ser estendido aos demais policiais, sobretudo aos agentes de polícia, pois muito ainda desconhecem os caminhos para obter os dados das principais redes sociais. Além de uma capacitação que alcance o maior número de policiais possível, deveria ser formado um grupo de estudos para a elaboração de um manual contendo orientações (passo a passo), modelos de ofício e outras informações necessárias para solicitar tais dados às redes sociais, bancos e outros aplicativos (Correia, 2023).

In this context, according to the head of the 8th DEAMV in the city of Porto Nacional/TO:

> Já tive outro caso (de tentativa de estupro, praticado por meio de mensagens de aplicativo) em que foi necessário solicitar quebra de sigilo para obtenção de dados de conexão, e somente logrei êxito na diligência após solicitar a ajuda de uma colega que já trabalhava na área de crimes cibernéticos, que me orientou tanto na fase do pedido judicial, como também na análise dos dados, pois realmente é algo que foge ao trabalho cotidiano da delegacia (Correia, 2023).

In addition, according to Dr. Fernanda, police officers who work in call centers should also receive this training, especially so that they can include in the police reports all the information needed to support the investigation, as well as immediately request the preservation of content on the respective platform.

5.1.2 Virtual rape in the city of Miracema/TO

In the city of Miracema/TO, according to Toledo (2018), an investigation led by the Police Station Specialized in Cybercrime Repression of the city of Palmas in the State of Tocantins (DRCC) led to the arrest of a man for committing rape in the virtual environment.

According to the investigation, a 23-year-old man had used social networks with a fake profile to contact the victim, a 22-year-old woman, in which he asked her for intimate photos, and the victim complied with the requests of the suspect for a certain period of time. However, the victim decided not to send any more photos or videos, which led the suspect to blackmail her because if she didn't send him new videos and photos, he would release all of the intimate content of the victim, which was in his possession.

According to Dr. Milena Santana, head of the Specialized Cybercrime Repression Police Station, at the time of the incident, the victim gave in to the threats made by the suspect, but later asked the Civil Police for help. The crime was confirmed by technical evidence and later prosecuted in the District of Miracema do Tocantins, where the suspect lived, and a search and seizure warrant was served at his home, where his cell phone was seized.

In the words of the head of the Police Station Specialized in Cybercrime Repression[3], regarding the difficulties faced in the investigation: "Most of the digital evidence had been deleted by the victim. The Internet connections used were via IP address, with CGNAT". It is therefore clear that identifying the perpetrator solely by the IP address assigned to the terminal from which the crime originated was insufficient, given that it was an IP address of the IPV4 type, shared publicly via CGNAT, which makes the investigation extremely difficult.

With regard to the techniques used, Dr. Milena points out that telematic data, registration data and respective links were analyzed, along with field survey work. With regard to the investigative method used, the head of the Specialized Cybercrime Repression Police Station states that: "The methodology was appropriate, within the working conditions experienced at the time, resulting in the identification of criminal authorship and materiality."

Finally, in the words of the delegate:

[3] Entrevista concedida por Milena Santana de Araújo Lima, em 4 de agosto de 2023. A Sra. Lima, na época da investigação em epígrafe, era delegada-chefa da Delegacia de Repressão a Crimes Cibernéticos (DRCC), na cidade de Palmas/TO. Atualmente está lotada na Divisão de Inteligência do Núcleo de Inteligência e Segurança Institucional do Tribunal de Justiça do Estado do Tocantins.

> As pessoas têm, em geral, a ideia de que o anonimato é intangível pela Internet, que na realidade não é, então tudo que você faz pela Internet deixa rastros. A investigação de crimes cometidos em meio eletrônico, pode ser mais complexa, pode ser mais extensa, mas não impede a identificação da autoria delitiva, nem a sua responsabilização penal" (Santana, 2023).

5.1.3 Joint operation by the Civil Police of the States of Bahia and Tocantins

According to Cruz (2021), on April 5th, 2021, in a joint operation by the Civil Police of the States of Bahia and Tocantins, a warrant was served for the arrest of a 20-year-old man suspected of committing virtual rape of children and adolescents. When the warrant was served, cell phones containing images and videos of the victims were seized.

Dr. Claudemir Luiz Ferreira, Deputy Police Chief of the Cybercrime Squad at the time, explains that the suspect used more than 80 fake profiles on the social network Instagram: "He started conversations with children and teenagers, obtained intimate photos and videos of the victims and then blackmailed them into continuing to show off sexually for him." The investigations found that the man had victims in the States of Tocantins, Minas Gerais, Ceará, among others.

With regard to the challenges and difficulties faced in the course of the investigations into this case, Dr. Claudemir[4] clarifies:

> O caso em questão talvez tenha resultado na primeira prisão e indiciamento pela prática, em tese, do crime de estupro na modalidade virtual no Estado do Tocantins. Aqui vale destacar que a equipe da DRCC – Palmas era e é muito qualificada, e todos se dedicaram ao caso. Acho que a grande dificuldade e desafio no processo investigativo foi demonstrar ao judiciário a necessidade e importância de medidas cautelares (quebras de sigilo telefônico, telemático e prisão) do investigado, pois mesmo estando a milhares de quilômetros da vítima, o autor lhe causava grande sofrimento psicológico (Ferreira, 2023).

With regard to the techniques and tools used to find the perpetrator, the Deputy of the Cybercrime Squad explains that the investigation was based on the data obtained through the breach of confidentiality, as well as the real-time

[4] Entrevista concedida por Claudemir Luiz Ferreira, em 9 de agosto de 2023. O Sr. Ferreira, na época da investigação em epígrafe, era delegado adjunto da Delegacia de Repressão a Crimes Cibernéticos (DRCC), na cidade de Palmas/TO. Atualmente ocupa o cargo de delegado-geral da Polícia Civil do Estado do Tocantins.

monitoring of telephone calls, which resulted in the identification of the suspect and his location in the State of Bahia, preventing new criminal acts from being perpetrated by the individual, noting that he was simultaneously embarrassing a teenage girl from the State of Minas Gerais through threats.

In addition, with regard to what could be improved in the investigation of crimes of this nature, in the methodological field developed by the Judicial Police of the State of Tocantins, Claudemir (2023) points out that: "In light of the investigation carried out, in which the data analysis process was practically done manually, today I am convinced of the importance and need to invest in technology in order to facilitate and streamline the work of investigators."

In the same vein, the police authority stressed the importance of an institutional effort to raise awareness among the civil police officers of the State of Tocantins, with a view to gain sufficient knowledge in the field of investigating crimes committed in the virtual environment, which would be of fundamental importance for unraveling not only virtual crimes themselves, but also many others that use cyberspace as a springboard for the operation of the most diverse criminal conducts.

5.2 Cyber Forensics of Virtual Rape in the State of Tocantins

The investigation of sexual crimes committed through the virtual environment requires an improved system of criminal forensics aimed at extracting and preserving digital evidence, especially after the inclusion of the chain of custody system in the Code of Criminal Procedure, inaugurated in Brazilian criminal procedural legislation with the entry into force of the Law No. 13,964 of 2019 (Anti-Crime Package). At this point, we will analyze important procedural aspects of criminal forensics in the context of investigations into virtual sex crimes.

The technical expertise of the Civil Police of the State of Tocantins, in the collection of digital traces, goes through a number of stages: a) Identification; b) Isolation; c) Collection; d) Preservation (forensic duplication and hashes); e) Processing (data carving); f) Analysis; g) Reports. We will analyze these stages below, using as a basis the information provided by criminal expert Leila Diniz, head of the Forensic Computing Center of the Civil Police of the State of Tocantins[5].

[5] Entrevista concedida por Leila Diniz Alves, em 20 de junho de 2023. A Sra. Alves é perita-chefa do Núcleo de Computação Forense da Polícia Civil do Estado do Tocantins.

The initial procedure in the identification phase consists of Post Mortem Analysis or Live Analysis. In the former, the analysis and extraction procedures are carried out on non-volatile storage media, such as: a) hard disk, external hard drive, pen drive, DVDs, CDs, among others. With regard to the second, it should be noted that some digital evidence will only be obtained if the electronic device's operating system is switched on, whereby data stored in RAM, for example, will be lost if the device is switched off.

The next step is forensic duplication, which is a reliable copy of the original "bit for bit" of the digital evidence, by blocking the writing of the evidence, using the hash algorithm to ensure integrity in the process.

The following tools are used for this duplication: Encase Imager, FTK Imager and TD3 Forensic Imager (Tableau) and Hasher to generate the hash algorithm. As Leila (2023) explains: "Processing is carried out on the duplicate images using techniques such as data carving (recovery of deleted files) and data indexing."

Figure 5: TD3 *Forensic Imager* (*Tableau*)

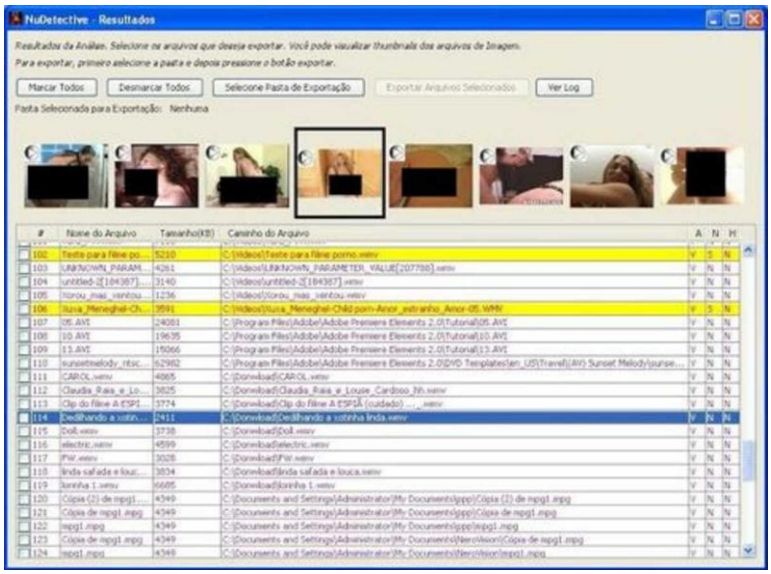
Source: Officer, 2023.1

Furthermore, the processing of duplicate images also uses OCR (Optical Character Recognition), a technology used to recognize and extract texts from various sources, compare hashes and so on.

With regard to data processing and analysis, criminal experts of the State of Tocantins use the IPED (Indexer and Processor of Digital Evidence) expert tools, Magnet Axiom and Autopsy software, for searching and analyzing Internet artifacts, and UFED Physical Analyser (especially for mobile devices, such as cell

phones). In the case of child pornography, tools are also used to help detect nude images, such as NuDetective and the Digital Evidence Locator (LED).

Figure 4: NuDetective System



Source: "Correio do Estado", 2023.1

Computer forensics, when analyzing child pornographic content, uses image classification techniques, categorization, markers and indexes. Once the analysis has been completed and the resulting data is available, reports will be generated to support the investigation. In the case of UFED, as explained above, the reporting tool is the UFED Reader.

The use of these cyber forensics techniques and tools has achieved important successes and results at the heart of investigations of a certain nature: a) Operation Light of Childhood (the largest operation to combat crime against the sexual dignity of children and young people on the planet), which was launched in several phases, the first of which was 100% effective, in which all the targets were arrested in the act; b) Operation Dark Net, which resulted in the arrest in the act of a doctor in the city of Peixe/TO, where the team of criminal experts from the State of Tocantins participated directly.

According to data provided by the Civil Police Computer Forensics Center of the State of Tocantins, between 2017 and 2022, cyber forensics techniques were used in sex crimes in several investigations, as follows: a) 93 cases of child pornography; b) 53 cases of rape of a vulnerable person; c) 32 cases of rape; d) 3 cases of sexual harassment. The unit also carried out 14 police operations in

support of the police stations of the State, with the aim of carrying out forensic examinations involving crimes against the sexual dignity of children and adolescents.

5 Challenges faced by the Judicial Police of the State of Tocantins in collecting digital evidence and tracking down criminals

With regard to aspects of the investigation, specifically in relation to the challenges faced by the Civil Police of the State of Tocantins in investigating sexual crimes committed in the cyber environment, especially virtual rape, Dr. Lucas Brito (2023), Chief Deputy of the Cybercrime Repression Division (DRCC), emphasizes the importance of expanding the police power of the Chief of request, in the words of the police authority: "The power of the Police Delegate of requisition is very restricted, as many investigations are plastered already at their inception, lacking data that can currently only be provided through judicial authorization."

In the same context, the head of the Cybercrime Repression Division highlighted the short deadlines set out in the Civil Mark of the Internet for the mandatory storage of connection and access logs by Internet connection and Internet application, essential data for investigations involving virtual sex crimes, including virtual rape. Another point raised by the delegate is the failure of application of the logical doors on the part of application providers:

> As portas lógicas são fundamentais na individualização de acessos realizados por meio do CGNAT (Carrier Grade Nate) – faixa dedicada às conexões via protocolo de rede no qual diferentes usuários compartilham simultaneamente o mesmo endereço IP – não são indicadas pelos provedores de aplicação (Santana, 2023).

Internet connection and application providers usually only provide the connection or access record, respectively, without providing the logical ports or even the MAC address, which are essential for identifying the terminal from which the crime was committed and which can identify the hardware used by the cybercriminal.

Another difficulty faced is the low level of collaboration on the part of some platforms, and even when they are judicially demanded, many of them provide unsatisfactory, incomplete or untimely responses. In addition, the low number of

civil police officers in Tocantins with specific qualifications for this area of activity has been a huge barrier to the success of cyber investigations in general, given that the number of police officers qualified for this task is very small, and the palliative solution of "practical" training for police officers who show some interest in the area of cyber investigation is commonly adopted.

Despite the valiant efforts of the Superior Police School (ESPOL) to offer training courses in the cyber area, according to the head of the Cybercrime Repression Division in the city of Palmas/TO, it is still insufficient; they should be offered on a regular basis, with the aim of improving and updating the profession. Similarly, the databases that the Civil Police have access to are obsolete and limited, and sometimes out of date.

The improvements pointed out by the interviewee include solving the problems presented, such as expressly extending the power of the Police Chief of request, in order to legally ensure the possibility of administratively obtaining some important preliminary data in cybercrime investigations, such as connection records for creating accounts/profiles and specific accesses. Another point is the need to increase the legal deadlines set out in the Civil Mark of the Internet, for the purposes of mandatory storage and provision of connection and access logs by Internet connection and application providers, and also the need for express provision regarding the mandatory storage and provision, within the legal interstices, of the logical port in accesses via CGNAT.

In addition, Santana (2023) highlights the need to impose civil, criminal and administrative sanctions on platforms that do not collaborate with investigations or recalcitrantly comply with the measures demanded, giving effect to the Article 12 of the Law No. 12,965 of 2014. It is also essential to train civil police officers to work in this investigative field, accompanied by the necessary professional development, from a salary and material/structural point of view. The police institution should periodically offer refresher courses on cybercrime investigation methods and tools, seeking out the professionals with the most expertise in each subject, as in the case of investigations into the crime of virtual rape.

Santana (2023) states that greater integration of systems and databases is a good idea, since the majority of targets in cybercrime investigations (even in the case of virtual rape) live in locations far from where the investigative unit is based, making it essential to search for their qualifications in official sources that are up-to-date and integrated with various databases, even local ones (energy and water utilities, health and education departments, etc.).

From the perspective of criminal forensics, as explained by the head of the Forensic Computing Center of the Civil Police of the State of Tocantins, there are a number of circumstances that contribute to the rapid growth and spread of virtual sex crimes. Initially, it is important to highlight the high complexity of the forensic examinations to be carried out, requiring highly specialized knowledge.

With regard to the mentioned investigative complexity related to technical forensics work, the methods of extracting data from electronic devices are an example of how a professional with advanced knowledge is required. With regard to extraction methods, we can list the following: a) manual (superficial); b) logical in the broad sense: logical level in the strict sense and file system level; e) physical; f) hex dump; g) chip-off; h) Join Test Action Group (JTAG); i) micro-reading.

In manual (superficial) extraction, there is no need to use any specific software; the data is accessed directly by handling the device, requiring only that the device is unlocked. In this method, it is impossible to recover deleted data.

Logical extraction in the broad sense requires the use of specific software, and it is subdivided into two types of extraction: a) logical level in the strict sense; b) file system level. In the first, the software interacts with the operating system of the device and it can extract several important data, such as SMS, contacts, call logs, media and audio. In the second, the software collects backup data from the device, as well as recovering hidden files, and it can extract images, videos and application content (Facebook, WhatsApp, Instagram, etc.).

Physical extraction is more in-depth, as it reaches the physical memory of the device and it is usually the only method that recovers data that has been deleted. Hex dump is a physical extraction method that uses software to directly access the contents of the flash memory of the device and recover deleted data. Flash memory is a computer memory chip that keeps information stored without the need for a power source.

Similarly, in the chip-off method of physical extraction, the extractor removes the memory chip from the board of the device and uses a chip reader to extract the data, which can cause physical damage to the device. This is a highly complex method, given that smartphones in particular have been showing encoding in the physical memory.

Another physical extraction method is the JTAG, which involves direct intervention in the device using solder on the circuit board of the device, providing access to raw information stored in flash memory. There is also the

micro-reading method, also a physical extraction method, which consists of reading each logic gate in the memory circuit under an electron microscope.

Analyzing the methods of extracting data from electronic devices explained above, it is clear that it is of the utmost importance for cyber investigative bodies to have specific tools and software at their disposal to carry out investigative work into sexual crimes committed in the virtual environment. On this point, criminal expert Leila (2023) states: "It is necessary to provide specialized tools and software and digital data storage resources, which requires a high level of investment".

In addition, the head of the Forensic Computing Unit of the Civil Police OF THE State of Tocantins stressed the volatility of digital information, which requires the use of technological means to preserve the content extracted and analyzed, especially with a view to preserving the chain of custody of digital evidence.

Finally, when asked about improvements that could be implemented to strengthen the investigation and fight against virtual sexual crimes, especially virtual rape, from the perspective of technical expertise, Leila (2023) stressed the importance of frequent training of experts working in the field, the acquisition of specialized tools and software, digital storage resources to facilitate access to reports by the actors involved in the investigation, prior filtering of evidence sent for expert analysis and the sharing of information between investigative actors and the expert team.

6 FINAL CONSIDERATIONS

The study carried out in this article has shown that the practice of virtual rape adapts to the criminal types of rape and rape of a vulnerable person, given that they are free-form offenses and that physical contact between the perpetrator and the victim is not necessary.

According to doctrine and case law, the crime of rape in cyberspace is fully possible, and there have already been judged cases in which the occurrence of virtual rape has been recognized, although there are some considerations regarding the virtuality of the sexual crime, as it would be real conduct practiced in a cyber environment.

Furthermore, with regard to the classification of virtual rape, we can conclude that the current legislation allows the crime to be committed in the cyber

environment, both in the art. 213 and the art. 217-A of the Penal Code, and there is no need to speak of a violation of the principle of strict legality.

However, as explained, it would be a good idea to improve the legislation, with a view to expressly providing for the commission of conduct in the cyber environment, which would bring more legal stability, as well as giving a modern wording to the mentioned legal provisions.

Sexual extortion practiced in the cyber environment, even if there is a lucrative (patrimonial) purpose, does not attract the incidence of the crime of extortion of a patrimonial nature, given that in the former the specific subjective element (special purpose of action) is the satisfaction of the lust of the perpetrator and practiced by means of a serious threat, it is immediately adapted to the criminal type of the crime of rape. However, it would be a good idea for the legislation to be improved, with a view to removing any doubt as to whether sexual extortion fits into the criminal types of rape and rape of a vulnerable person.

Furthermore, the investigation of sexual crimes committed in the virtual environment, especially virtual rape, has proved to be a major challenge for the Civil Judicial Police, and this is no different in the State of Tocantins, where problems are faced both in the investigative field and in the area of technical expertise, as explained in this scientific study.

However, as discussed above, the Civil Police of the State of Tocantins have developed important successful investigations into sexual crimes committed in cyberspace, in this case virtual rape, demonstrating expertise in the area of cyber investigation.

In addition, problems with the operationalization of digital trace collection and storage represent major barriers to the efficient protection of the health and integrity of the chain of custody of digital evidence, and investments are needed to improve expert performance.

With regard to the investigative field in the police of the State of Tocantins, there is a need to train police officers so that they can acquire technical and operational knowledge to work in the investigation of cybercrimes, including virtual rape, which has already been carried out through training led by the Superior Police School of the State of Tocantins (ESPOL/TO).

Furthermore, the expansion of the power of request of the police officer, together with greater speed and promptness in responding to requests for information from Internet connection and application providers, would be of

great relevance to investigations into sexual cybercrimes, especially in relation to virtual rape.

Therefore, the incidence of sexual crimes in the cyber environment, including virtual rape, is a contemporary reality of modern crime, which demands greater procedural and operational improvement on the part of investigative bodies, a demand that is present within the Tocantins Civil Police, which has sought to improve investigative techniques, either through training courses or through the use of tools and software aimed at unraveling crimes committed to the detriment of the sexual dignity of users of the large network.

REFERÊNCIAS

BRASIL. Superior Tribunal de Justiça. Recurso em Habeas Corpus 70976-MS. Rel.: Min. Joel Ilan Paciornik. Julgado em: 2/8/2016. DJe 10/8/2016.

CASELLI, Guilherme. Manual de Investigação Digital. 3. ed. São Paulo: JusPodivm, 2023.

CAVALCANTE, Márcio André Lopes. Contato físico entre autor e vítima não é indispensável para configurar o delito. Buscador Dizer o Direito, Manaus. Disponível em: <https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/1f3202d820180a39f736f20fce790de8>. Acesso em: 2/6/2023.

CUNHA, Rogério Sanches. Manual de direito penal: parte especial. 8. ed. Salvador: JusPodivm, 2016.

CRUZ, Shirley. Ação conjunta das polícias civis do Tocantins e da Bahia resulta na prisão de homem investigado por estupro virtual de crianças e adolescentes. Disponível em: https://www.to.gov.br/ssp/noticias/acao-conjunta-das-policias-civis-do-tocantins-e-da-bahia-resulta-na-prisao-de-homem-investigado-por-estupro-virtual-de-criancas-e-adolescentes/3y2lejo1fjom Acesso em: 13 ago. 2023.

TOCANTINS, Conexão. Polícia Civil indicia homem suspeito de praticar o crime de "estupro virtual" contra mulher em Porto Nacional. Disponível em: https://conexaoto.com.br/2021/10/08/policia-civil-indicia-homem-suspeito-de-praticar-o-crime-de-estupro-virtual-contra-mulher-em-porto-nacional Acesso em: 13 ago. 2023.

GONÇALVES, Victor Eduardo Rios. Direito Penal Esquematizado: Parte Especial. 8. ed. São Paulo: Saraiva, 2018.

GOMES, Matheus Arruda. Juiz do Piauí decreta primeira prisão por estupro virtual no Brasil. Jusbrasil. Disponível em: https://www.jusbrasil.com.br/noticias/juiz-do-piaui-decreta-primeira-prisao-por-estupro-virtual-no-brasil/493303189 Acesso em: 25 jun. 2023.

LOPES. Mariângela Tomé. A infiltração de agentes no Brasil e na Espanha. Possibilidade de reformulação do sistema brasileiro com base no direito espanhol. Revista Brasileira de Ciências Criminais. São Paulo, v. 19, n. 89, p. 495-532, mar./abr. 2011.

MARTINS, José Renato. Não é correto se falar em estupro virtual, o crime de estupro só pode ser real. Revista Consultor Jurídico, 2017. Disponível em: https://www.conjur.com.br/2017-ago-18/opiniao-crime-estupro-real-nunca-virtual. Acesso em: 4/6/2023.

MASSON, Cleber. Direito Penal: parte especial arts. 213 a 359-h. 8. ed. São Paulo: Forense, 2018.

MACHADO, Nealla Valentim; PEREIRA, Silvio da Costa. Sexting, mídia e as novas representações da sexualidade. In: Congresso Brasileiro de Ciência da Comunicação, 36., 2013, Manaus, Papers. Manaus: Intercom, 2013, p. 1 – 12. Disponível em: https://www.intercom.org.br/papers/nacionais/2013/resumos/R8-1134-1.pdf. Acesso em: 23 abr. 2023.

MEIRELES, Luciano Miranda. A realidade do Estupro Virtual. In. Revista Parquet em foco. n. 1. Escola Superior do Ministério Público do Estado de Goiás. Goiânia: ESMP-GO (set./dez. 2017).

PEREIRA, M.T.M.A. Investigação Policial de Crimes Eletrônicos. São Paulo: Acadepol – Academia de Polícia "Dr. Coriolano Nogueira Cobra", 2019.

PORTO, Márcio Rogério. Experiências positivas em investigações envolvendo compartilhamento NAT e CGNAT sem a porta de origem. In. Tratado de investigação criminal tecnológica. 3. ed. São Paulo: JusPodivm, 2023.

SATO, Gustavo Worcki. A infiltração virtual de agentes e o combate à pedopornografia digital. In. Direito Penal sob a perspectiva da investigação criminal tecnológica. 2. ed. São Paulo: JusPodivm, 2023.

SILVA NETO, Luís Gonzaga da. Investigação Criminal Tecnológica do Estupro Virtual. In. Direito Penal soba a Perspectiva da Investigação Criminal Tecnológica. Jorge, Higor Vinicius Nogueira (Coord.). 2. ed. São Paulo: JusPodivm, 2023.

SILVA, Andressa Benevides da. Estupro Virtual: análise doutrinária e jurisprudencial, 2020. Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/estupro-virtual-analise-doutrinaria-e-jurisprudencial/. Acesso em: 23 abr. 2023.

TOLEDO, Cleber. Suspeito de "estupro virtual" em Miracema é preso em Palmas. Disponível em: https://clebertoledo.com.br/tocantins/suspeito-de-estupro-virtual-em-miracema-e-preso-em-palmas/ Acesso em: 12 ago. 2023.

VALE, João Henrique do. Minas Gerais registra primeiro caso de prisão por estupro virtual. Jornal Estado de Minas, 21/09/2017. Disponível em: https://www.em.com.br/app/noticia/gerais/2017/09/21/interna_gerais,902256/minas-gerais-registra-primeiro-caso-de-prisao-por-estupro-virtual.shtml Acesso em: 25 jun. 2023.